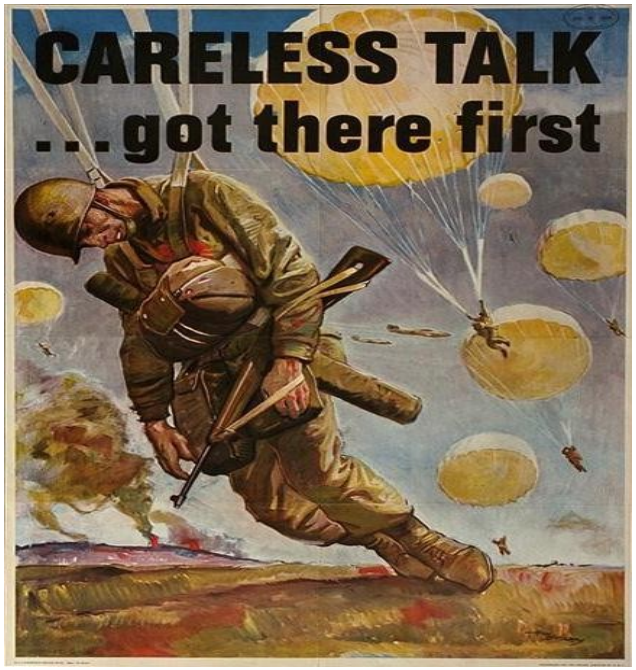
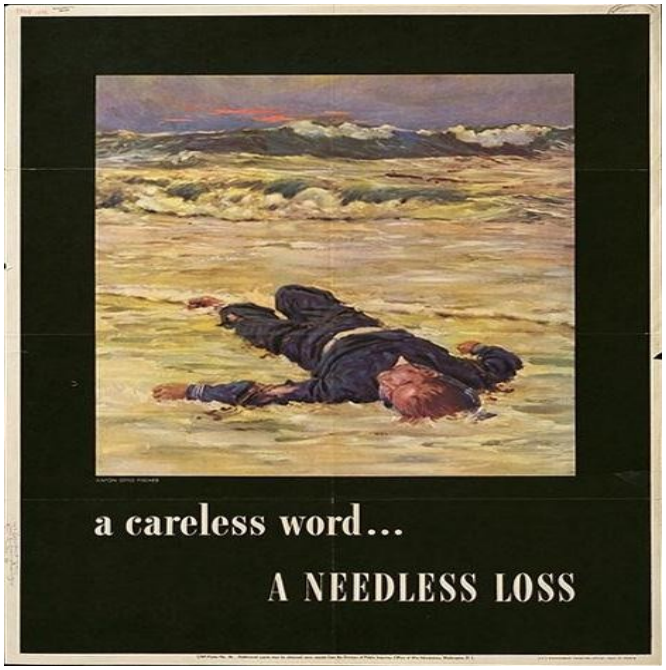
Operations Security (OPSEC)





435 ABW/86 AW OPSEC Officer: Lt Swaney

XXXXX Group or Squadron POC: XXXXXXX

U.S. AIR FORCE

OPSEC Defined

- **A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:**
  - **Identify those actions that can be observed by adversary intelligence systems.**
  - **Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive Critical information in time to be useful to adversaries.**
  - **Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploit**

Joint Pub 3-54

U.S. AIR FORCE

In General….

OPSEC IS
INFORMATION CONTROL
by

- knowing the threat
- knowing what to protect
- determine the risk &
- knowing how to protect your information!

OPSEC is not a Security Function…

U.S. AIR FORCE

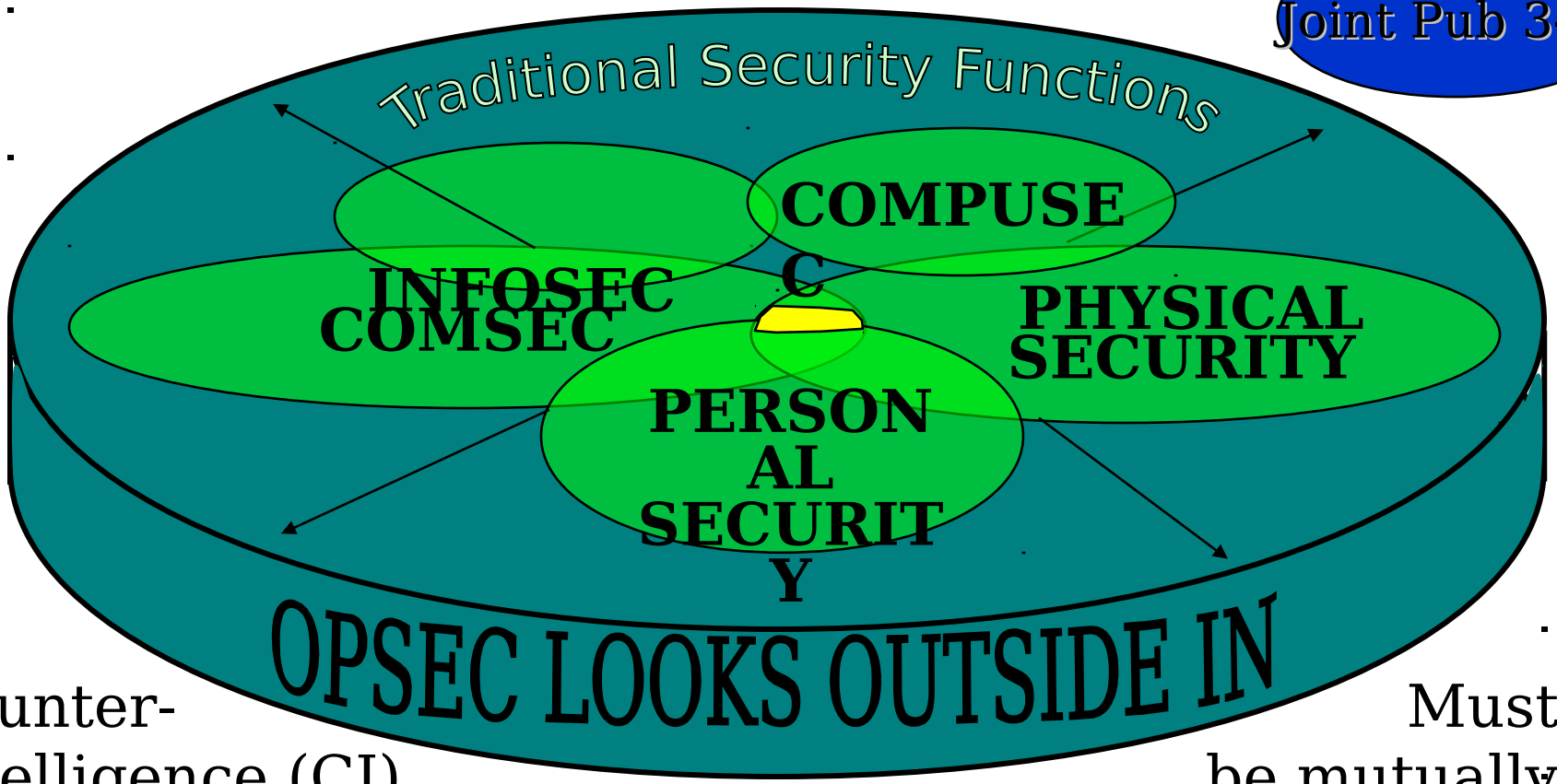
TRADITIONAL	OPERATIONS
• FOCUS ON PERSONNEL AND PHYSICAL SECURITY	• FOCUS ON OPERATIONAL EFFECTIVENESS
• ADDRESSES OVERALL MISSION	• FOCUS ON SPECIFIC ACTIVITY
• FOCUS ON CLASSIFIED INFORMATION	• IDENTIFIES AND PROTECTS ALL INFORMATION (Primarily unclassified) CRITICAL TO AN OPERATION, ACTIVITY, OR PROGRAM

…protects full Security of Operations!

U.S. AIR FORCE

OPSEC is an Operations Functional

Joint Pub 3-54



Counter-Intelligence (CI) supports both Security and OPSEC!

Must be mutually supportive to be effective!

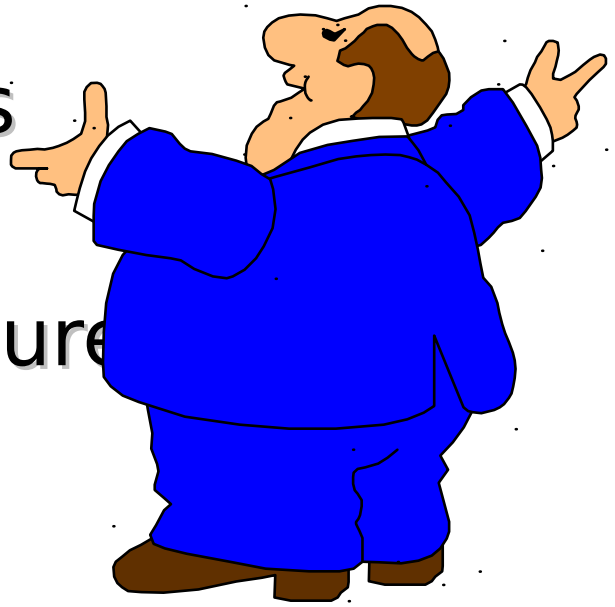
All Security must work together to provide Essen

U.S. AIR FORCE

OPSEC Methodology

Five Step Analytical Process

- Identify Critical Information
- Analyze Threat
- Analyze Vulnerabilities
- Assess Risk
- Develop Countermeasure



1. Know the threat!

ADVERSARY: ONE WHO…
CONTENDS WITH, OPPOSES, OR ACTS AGAINST
ANOTHER'S INTEREST

Not necessarily a traditional…
enemy or target!

Sleeper Agents?

Neighbors?

Diplomatic, military,
economic and information

"Courage"

U.S. AIR FORCE

THREATS

- **Over 90 countries actively collect intelligence information on the US.**
- ***Some* are considered allies of the US.**

U.S. AIR FORCE

Intelligence Gathering Methods

There are several different methods for gathering intelligence. These methods will be discussed in the following 4 slides.

U.S. AIR FORCE

Human Intelligence (HUMINT)

- **Mata Hari: Belgian national married to a Belgian Army Officer. Had contacts in high places. In the employ of Germany. Gave the Germans general military information. Executed by the French in 1917.**

U.S. AIR FORCE

Open Source Intelligence (OSINT)

- Commercial imagery
- Books and magazines (Jane's is excellent)
- Internet sites
- News media of all types

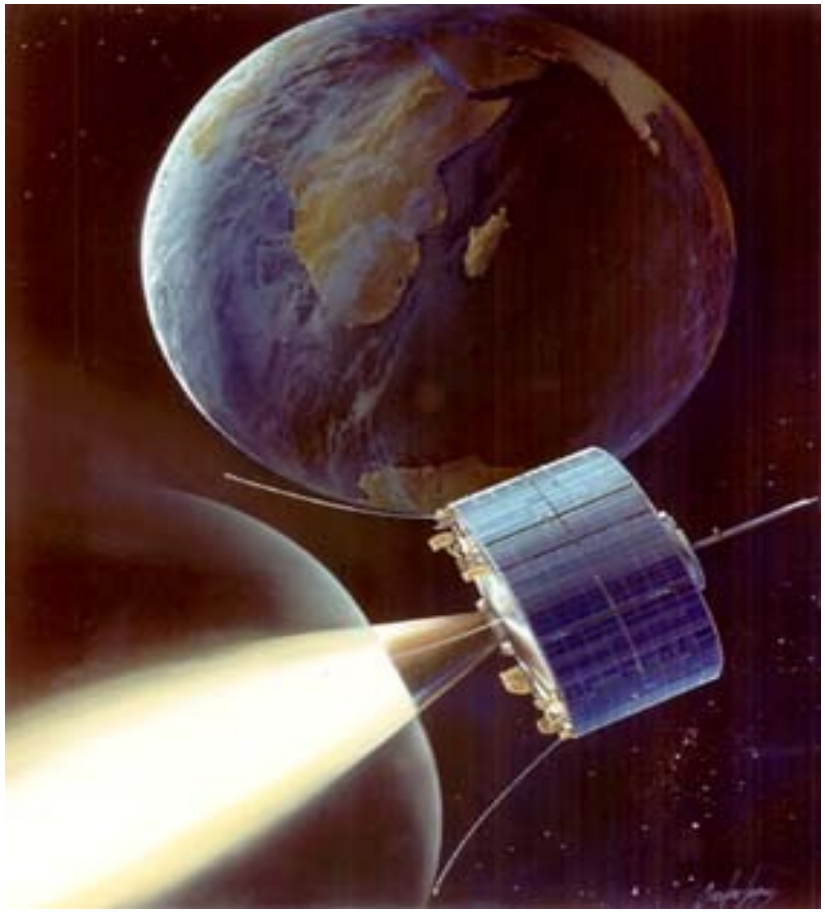
U.S. AIR FORCE

Signals Intelligence (SIGINT)

- **Overt collection through satellites, antenna fields, and airborne platforms.**
- **Covert collection through vans and bugs.**

U.S. AIR FORCE

Imagery Intelligence (IMINT)



- **Satellites**
- **EO Imagery**
- **Airborne Platforms**

U.S. AIR FORCE

...the THREAT has increased!

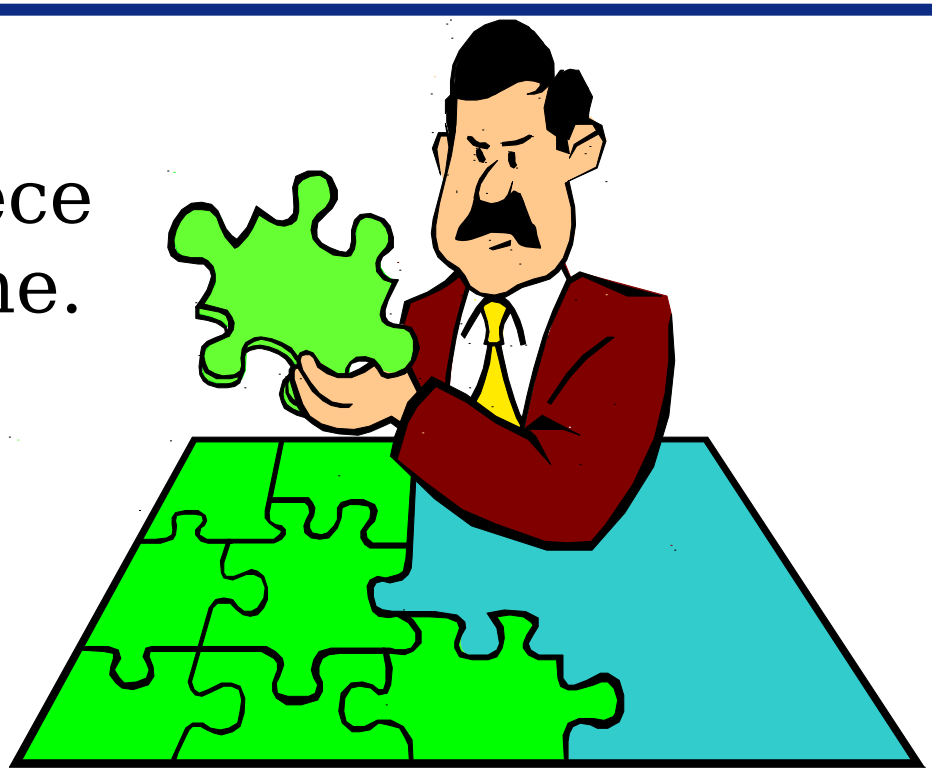
Terrorists

- Nation States
- Businesses
- Criminal Networks
- NG Organizations
- Hackers/Crackers
- Individuals

What is the Adversary's Goal?

U.S. AIR FORCE

One piece at a time.



What piece is the final piece?

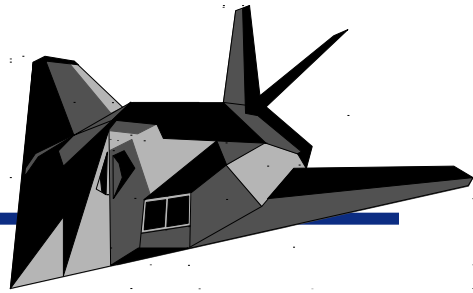
Patience!

Persistence!

To put together enough pieces to solve the Puzzle!

U.S. AIR FORCE

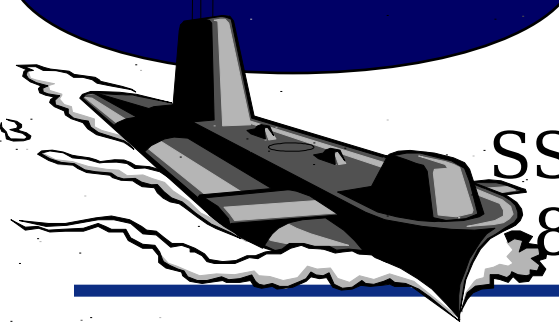
2. Know your Critical Information



Specific facts about friendly intentions, capabilities and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for f[illegible] mission accomplishment. (Joint

Classified or Unclassified

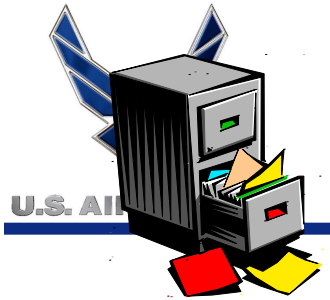
How we protect our information



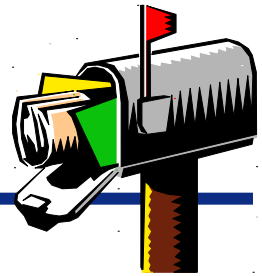
"Anything we'd like to know about our enemy, our enemy would like to know it about us."

SSBN arrives Point Charlie at 0400Z.

82ND Airborne cancelled all leaves.

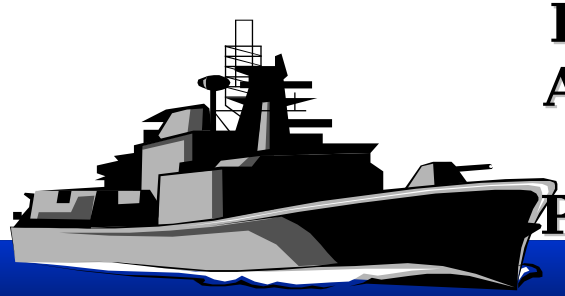


2a. OPSEC Indicators (what can be seen):

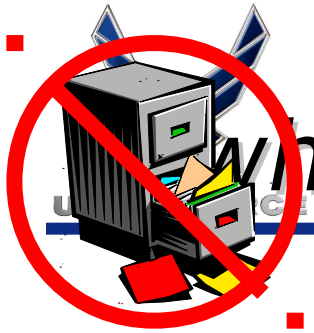


Friendly <u>detectable actions</u> and <u>open source information</u> that can be interpreted or pieced together by an adversary to derive <u>critical information</u>

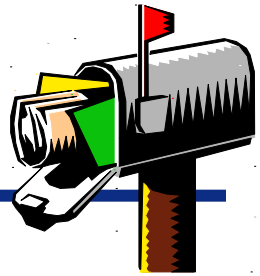
(Joint Pub 1-02)



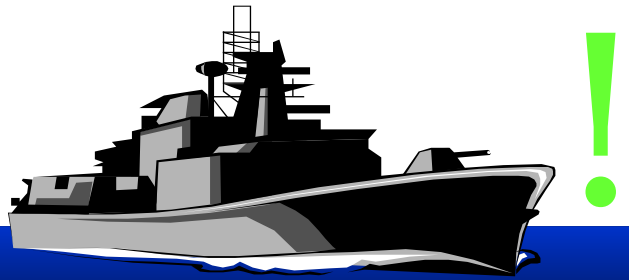
***NOT ALL INDICATORS ARE BAD OR REQUIRE PROTECTION**



3. OPSEC Vulnerability (what can be collected upon):



A condition in which <u>friendly actions</u> provide <u>OPSEC indicators</u> that may be obtained and accurately evaluated by an adversary in time to provide a basis for <u>effective</u> adversary decision making (Joint Pub 1-02).



U.S. AIR FORCE

Known Vulnerabilities – where they can collect!

- Cell Phones_
- Pagers &

PDAs

- Telephones
- ULAN Web-

sites

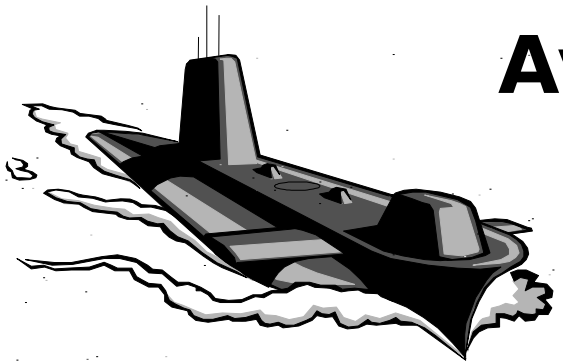
"Courage"

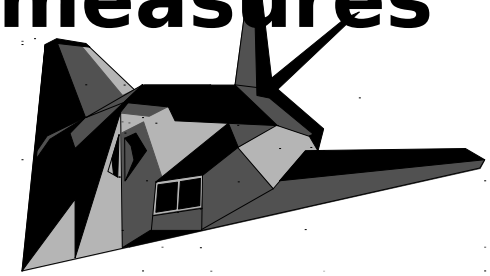
435 ABW/86 AW Critical Information List

- **Daily Operations**
- **Command, Control, Communication, Computers, Intelligence (C4I)**
- **Force Protection, Personnel, Administration, Logistics**

-See Full List

Available Countermeasures





435 ABW/86 AW Critical Information List

Daily Operations

Military capabilities
Forces assigned and deployed to Ramstein
Force composition and disposition
Logistic capabilities and limitations
Origin and destination of equipment being moved
Flight planning
Foreign overflight arrangements
Origins/destinations
Memorandums of agreement
Automatic (IFF) codes

See Unit OPSEC POC For Unit-Specific CIL!!!

Command and Control

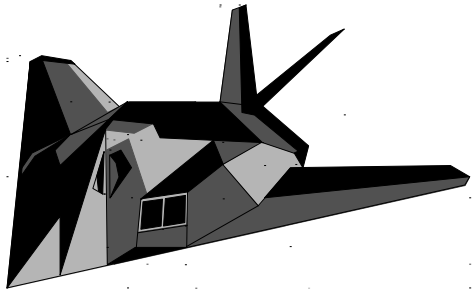
Location of critical C2 nodes
C3 connections and weaknesses
C2W support and capabilities
Movement of key personnel
Exercising

Logistics

Capabilities and constraints
Fact of weapons movement
Periodicity of movement
Origin and destination of equipment being moved
Extent of inventory of equipment being moved

Surges

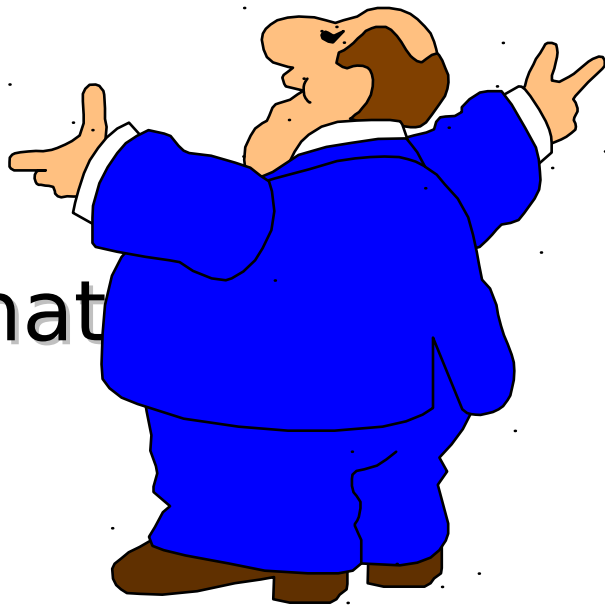
OPlans, contingencies that are actual or exercised



U.S. AIR FORCE

Countermeasures

- Instilling the right mindset
- Assume the enemy is listening
- STU III or STE
- SIPR
- Limitation of your imaginat



U.S. AIR FORCE

BASIC GUIDLINES

1. Shred 100% of all paper with the exception of magazines
and newspapers

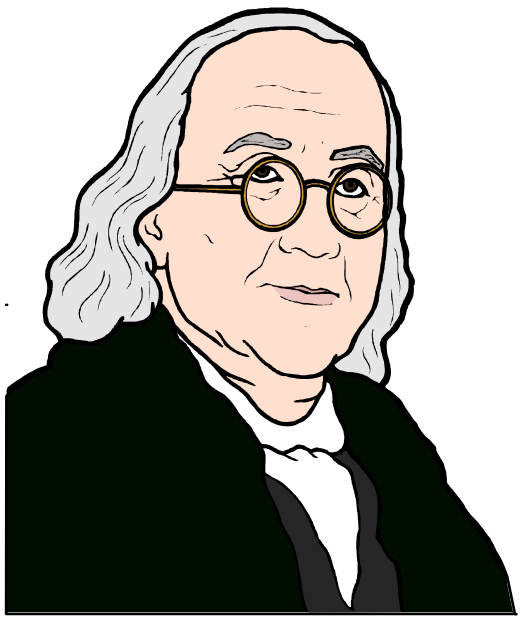
2. Use the “OPSEC Check” mental button before sending an e-mail. Information from Critical Information Lists (CIL) may be discussed via the NIPRNET when restricted to the ramstein.af.mil domain. However, information sent to addresses outside the base firewall is more vulnerable to interception, thus e-mails containing CIL data must be communicated via the SIPRNET. Remember this simple rule: “If you wouldn’t say it over the phone, don’t say it in an e-mail.” Finally, at no time will mission related information be sent to personal e-mail addresses.

U.S. AIR FORCE

BASIC GUIDLINES

3. Adhere to USAFE's electronic device policy dated 4 Aug 2000 which states: "Cellular phones, two-way radios, beepers and any other electronic equipment that can receive and transmit a signal are prohibited in all staff offices where sensitive information may be discussed."

4. Restrict mission related communication to secure methods (STE or SIPRNET) and areas. In other words, leave work at work. Personal web pages, restaurants and nightclubs are not secure environments, however, they are prime targets for our adversaries to obtain desired information.



“If you want to keep a secret, tell it not to a friend”

-Benjamin Franklin